



OSINT + ARCO + PROTECCIÓN DE DATOS

MAPA-RD: Exposición y Ruta de Cierre

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

ACME Corp · Reporte RPT-2026-001 · 2026-01-11

Executive Security Report · Exposición pública · Confidencial

Índice de Riesgo Digital

65

RIESGO CRÍTICO

VECTORES DE VULNERABILIDAD

VEC-001	Exposed Database Credentials	85 MÁXIMO
ACTIVO:	TIPO:	EXPOSICIÓN:
Production Database (AWS RDS)	Cloud Infrastructure	Public Repo Leak
DESCRIPCIÓN DEL EVENTO		RUTA DE CIERRE
<p>Hardcoded credentials for the primary production database were identified in a public GitHub repository (config.js). Determining access logs confirmed unauthorized clone events.</p>		<ol style="list-style-type: none">1. Revoke the exposed AWS IAM credentials immediately.2. Rotate the database master password.3. Audit CloudTrail logs for suspicious activities since the commit date.4. Implement git-secrets to prevent future commits.
IMPACTO		<ul style="list-style-type: none">• Full compromise of customer data (PII).• Potential total service disruption (Ransomware).• Severe regulatory fines (GDPR/CCPA).

VEC-002

Admin Portal without MFA

60 CRÍTICO

ACTIVO:

admin.acme.com

TIPO:

Web Application

EXPOSICIÓN:

Missing Control

DESCRIPCIÓN DEL EVENTO

The administrative panel allows single-factor authentication. Brute-force attacks or credential stuffing could easily compromise an admin account.

RUTA DE CIERRE

1. Enforce MFA (Time-based OTP) for all admin roles.
2. Restrict access to VPN or trusted IPs only.
3. Implement rate-limiting on the login endpoint.

IMPACTO

- Unauthorized administrative access.
- Data manipulation or deletion.
- Backdoor installation.

VEC-003

Outdated SSL Certificate

35 MEDIO

ACTIVO:

dev.acme.com

TIPO:

Dev Environment

EXPOSICIÓN:

Configuration

DESCRIPCIÓN DEL EVENTO

The SSL certificate for the development environment is expired, triggering browser warnings and exposing traffic to interception.

RUTA DE CIERRE

1. Provision a new LetsEncrypt certificate.
2. Automate renewal via Certbot.

IMPACTO

- Developer workflow disruption.
- Man-in-the-Middle (MitM) risk if used externally.
- Loss of trust validation.

Anexo Técnico

METODOLOGÍA DE RIESGO V1.0 (OFICIAL)

1. Índice de Riesgo del Vector (IRV)

El **IRV** mide la urgencia y el impacto real de no remediar un vector de vulnerabilidad específico. Se calcula internamente mediante un modelo ponderado de seis dimensiones y se normaliza a una escala centesimal (0-100).

FÓRMULA GENERAL

$$\text{IRV} = [\Sigma (\text{Componente} \times \text{Peso}) / \Sigma (\text{Pesos Max})] \times 100$$

Variables del Modelo

CA (x4)

Criticidad del Activo. Evalúa la importancia del sistema afectado para la operación.

ET (x3)

Exposición Temporal. Determina si el hallazgo es histórico, residual o vigente.

SE (x3)

Superficie de Exposición. Mide la facilidad de acceso (Público vs Interno).

IM (x4)

Impacto Multidimensional. Suma binaria de impactos (Legal, Financiero, Operativo).

FE (x3)

Facilidad de Explotación. Nivel de esfuerzo técnico requerido por el atacante.

DV (x3)

Detectabilidad. Probabilidad de que el ataque pase desapercibido.

2. Índice de Riesgo Digital (IRD)

El **IRD** representa el estado global de riesgo de la organización. Es un indicador dinámico derivado exclusivamente de los IRV activos, utilizando un promedio ponderado por severidad.

CÁLCULO PONDERADO

$$\text{IRD} = \Sigma (\text{IRV} \times \text{Peso_Severidad}) / \Sigma (\text{Pesos_Severidad})$$

ESCALA DE SEVERIDAD (PESOS)

BAJO

Peso x1

MEDIO

Peso x2

ALTO

Peso x3

CRÍTICO

Peso x4

MÁXIMO

Peso x5

Este documento es confidencial y parte integral del entregable MAPA-RD. La metodología v1.0 es propiedad intelectual cerrada.

Protegiendo la información que importa